

FAS Standing Committee on Information Technology
Wednesday, November 6th, 1:00pm-2:30pm
Science Center 300H

AGENDA

1. Next steps on video pain points (Anne)
2. Recap and follow up from discussion with David Barron
 - a. Discussion questions
 - i. What is the right balance between providing access to data for academic planning and protecting individual privacy (i.e. data mining within Harvard community)?
 - ii. Are there principles this committee could articulate to guide that balance?
 - b. Open areas for discussion
 - i. Chief Privacy Officer
 - ii. Notice
 - iii. Audit/reporting
 - iv. Protocols for minimization of data access
 - v. Code of conduct for IT staff

FAS SCIT Discussion with David Barron

Friday, November 1, 2013

Attendees: David Barron, David Malan, Harry Lewis, Jim Waldo, Anne Margulies, Peter der Manuelian, Leah Rosovsky, Katie Vale, Henry Leitner, Greg Morrisett, Jay Harris, Howard Georgi, Valerie Beilenson

I. Overview:

- i. *Committee:* Chaired by David Barron (HLS), 14 members (representatives from each school) plus the CIO (Anne Margulies), OGC (Bob Iuliano), VP for Strategy and Programs (Lead Rosovsky) & VP for Human Resources (Marilyn Hausammann)
- ii. *Goal:* Recommend rules for obtaining access to electronic information by the university without the consent/knowledge of users
- iii. *Product:* Narrative report and a useable policy proposal
- iv. *Timeline:* Aiming to have work finished by end of January

II. Issues being addressed

- a. What are the stages of the decision to give access to user information?
 - i. Justification (what is the need for access)
 - ii. Authorization (who makes the decision that access can be granted)
 - iii. Conduct (how is the search conducted)
 - iv. Audit/notice (how and when is the search reported to the user and/or the community)
- b. Some characteristic situations in which access is needed
 - i. Business continuity (usually at the staff level)
 - ii. System maintenance and operations
 - iii. Legal demand
 - iv. Academic misconduct
 - v. Internal investigations—these are the most complex situations and typically lie outside of traditional committee contexts

III. Principles for recommendations

- a. Candor—being straightforward about the access that the university has
- b. Academic freedom/free inquiry
- c. Trust—ensuring that people feel comfortable using the system

IV. Open questions

- a. Who makes the judgment about when to do a search? Should it be individual deans, HUIT, the OGC, or an independent actor? If it is an independent actor who should that be? A new standing committee? An ombudsman? The head of an already existing committee? If outside eyes are needed, should that happen before or after the fact?
- b. When does notification need to happen—before or after? Are there certain cases in which notifying the user is not advisable?
- c. How do you define who has been searched such that they need to be identified?
- d. Should audits be available to the entire community? What if the numbers are so small that even revealing aggregate information is not enough to protect confidentiality?
- e. How should the community be notified of the policy once it is adopted? Pop ups? Reminders at each log-in? A post on a website?
- f. Should there be one policy for the whole university? Or should we divide it by school/component or role?
- g. What is the university's mechanism for dealing with unanticipated issues that arise? A Chief Privacy Officer?